

## 加餐4 | 个人成长：学习安全，哪些资源我必须要知道？

2020-02-21 何为舟

安全攻防技能30讲

[进入课程 >](#)



讲述：何为舟

时长 10:20 大小 8.29M



你好，我是何为舟。欢迎来到安全专栏的第四次加餐时间。

安全涉及的知识面非常广，更新速度也很快，前辈们很难有足够的时间和精力来言传身教。这个时候就需要我们具备良好的自学能力，通过持续地学习来掌握新的知识，应对新的变化和挑战。

优质的学习资源是自学的重要基础。今天，我就来盘点一下，对我个人的安全学习产生帮助的各类学习资源，以及不同阶段的安全人员应该如何对各类资源进行取舍。

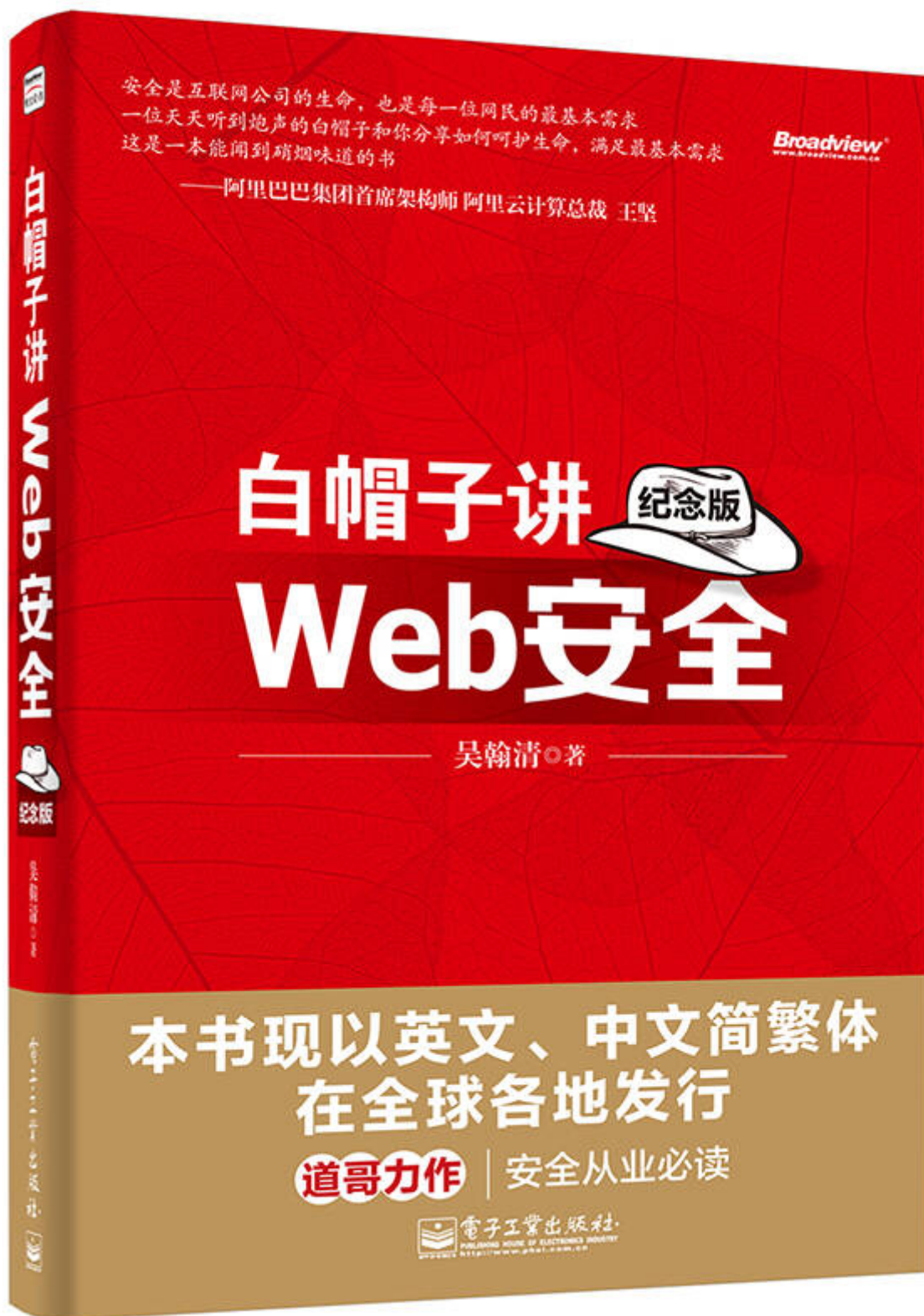


### 安全入门书籍

安全的核心能力分为两个方向：攻击和防御。俗话说“未知攻焉知防”，所以，学习安全一定是从攻击手段入门，在掌握了一定的攻击基础之后，我们再考虑选择某一个方向深入学习。

所以，我建议**刚入门的同学可以先选择几本攻击方向的经典书籍来学习。**

《[🔗](#)**白帽子讲 Web 安全**》这本书是大部分人的安全入门书籍。它覆盖了绝大部分的安全攻击知识，而且作者把知识点讲解得清晰，即使你没有安全基础也能很好理解。可以说，在学习完这本书之后，你已经具备了安全人员所需要的全部基础知识。



如果说《白帽子讲 Web 安全》是一本入门教程，那《 黑客攻防技术宝典》就是一本攻击手册。虽然同样是讲 Web 安全攻防内容，但是《黑客攻防技术宝典》对其中涉及的每一个细节和原理（如 HTTP 协议，浏览器技术等）都进行了详细讲解。你在学习 Web 安全的过程中遇到的大部分问题，都可以通过翻阅这本书来解决。因此，我建议你通读这本书，并且结合实际工作中遇到的问题随时查阅。

TURING 图灵程序设计丛书 网络安全系列



The Web Application Hacker's Handbook

Finding and Exploiting Security Flaws Second Edition

# 黑客攻防技术宝典

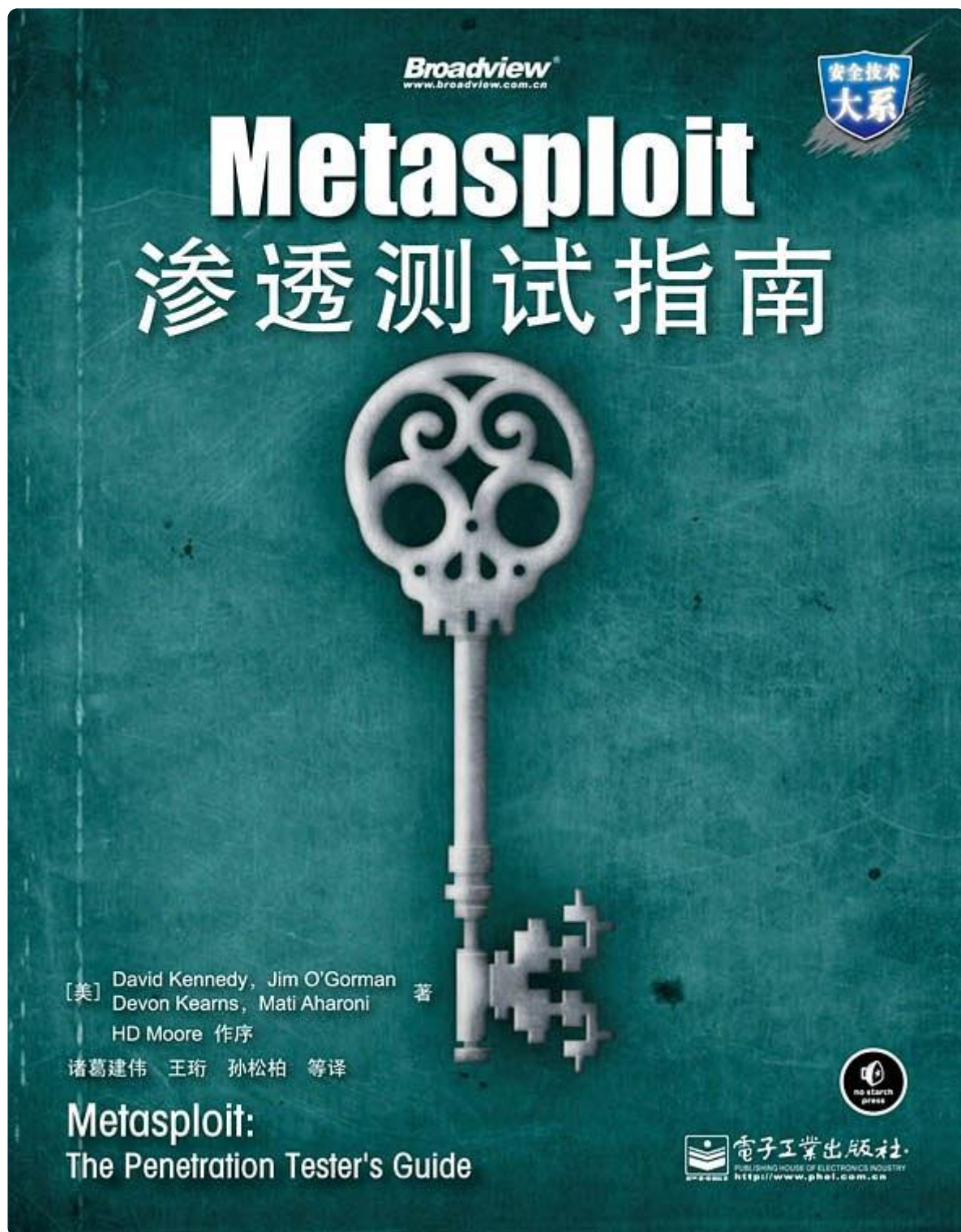
## Web实战篇 (第2版)



[英] Dafydd Stuttard 著  
Marcus Pinto  
石华耀 傅志红 译

人民邮电出版社  
POSTS & TELECOM PRESS

熟练使用各种渗透测试工具是安全攻击的必备技能，Metasploit 是最为常见的渗透测试工具之一。《[Metasploit 渗透测试指南](#)》这本书是学习这款工具最经典的书籍之一，书中对如何利用 Metasploit 发起各类攻击测试，进行了详细介绍。如果你想要快速掌握 Metasploit 的使用方式，这本书能够帮到你。



学完这几本书，你不一定能发起一次真实的攻击。但当你面对任何一起攻击事件时，一定能知道它的原理是什么。这恰恰就是所有安全人员需要具备的基础能力。

## 攻击进阶练习

有了一定的攻击基础之后，如果你还想向攻击渗透方向深入钻研，那就不是任何一本书能够解决的了。这个时候实战训练能够帮助你快速成长。下面，我就来分享一些我觉得很实用的攻击渗透平台。

🔗 **WebGoat**是最权威的 Web 安全组织 OWASP 提供的一个 Web 安全练习平台，它几乎涵盖了全部的 Web 安全漏洞的讲解和练习内容。使用 WebGoat 有两大好处：首先，它是一个本地的平台。这意味着你可以随时查看网页的源码，甚至进行调试。因此，你可以清晰地了解一次攻击发生时，Web 应用内部到底发生了什么；其次，其中的每一个练习内容都有对应的知识讲解。所以，这个平台对你明确攻击方向，进行安全入门训练是十分适合的。

🔗 **Pwnable.kr**是我体验过的免费的攻击渗透平台中最好用的一个。Pwnable.kr 中的题目更偏向系统和应用层的攻击渗透（这些都是权限提升过程中的常见手段），适合用来进行攻击渗透的进阶训练。Pwnable.kr 的好用之处就在于，它提供了一个可以直接访问的 Linux 系统环境，省去了你在本地搭建环境的繁琐过程。

但是 Pwnable.kr 有一个缺点，就是不提供任何解题思路 and 答案，不过，网上已经有很多人公开了平台上题目的解题思路，你可以用来参考。但是，我还是建议你至少花 2-3 天的时间去思考和解决一道题目，如果仍然得不到结果，再去参考别人的答案。

如果自我训练已经无法让你获得成就感了，那是时候去参加一些比赛了。目前，国内的 🔗 **XCTF 联赛**最为知名。你可以独自作战，也可以叫上几个朋友组团参赛。

通常来说，一场 CTF 比赛会进行 48 小时以上，如果你精力充沛的话，可以去体验一把挑战极限的快感。而且，比赛方通常会在赛后公开部分题目的解题思路，你也可以拿来作为学习的资源。通过不断参加比赛，你可以磨练自己的攻击技巧和能力。除此之外，如果获得了足够的积分和名次的话，也是证明你个人能力的一个有力证明。

当具备足够的攻击能力之后，你既可以成为安全渗透人员，为企业应用的安全贡献力量，也可以成为一名“白帽子”，专门去挖掘各个公司的安全漏洞，然后提交给对应的 SRC，获取各类物质奖励。

## 企业防御书籍

如果你选择的是安全防御方向，你会逐步接触到公司的安全防御工作。那么在一开始，你一定要去学习各大公司的安全负责人的经验，看看他们的安全建设思路是怎么样的，以及有哪些“坑”需要注意。阅读他们的书籍，就是向大佬学习的一种最简单、快捷的方式。

有关企业安全的书，我读过比较好的有：赵彦的《[🔗互联网企业安全高级指南](#)》、聂君的《[🔗企业安全建设指南](#)》、石祖文的《[🔗大型互联网企业安全架构](#)》。这些书中有很大部分内容是相似的，从任何一本书中，你都能够了解到企业安全体系建设所需要使用的工具。对我个人来说，书中最精华的部分是作者对安全体系建设的思考、对各类安全工具的理解。



这些书的相似内容很多，读起来也不会花太多时间，所以，我建议你将这些书都读一遍。而且这些书籍都是安全行业内鼎鼎有名的大佬们，基于他们自己的防御体系建设经验总结而成的。虽然你不可能完全照搬里面的安全建设方案，但你可以从中吸取经验教训，博取众家之长，然后设计出适合你们公司的最佳方案。

## 安全证书

除了书籍和练习平台，我还想和你分享一些比较有价值的安全证书。以我了解到的现状，这些证书对应聘安全工作不会有太大的帮助。但我认为，这些证书最大的意义就在于，它能够推动你对安全知识体系进行补充和整理。因为考证的过程也是你对学过的知识，进行再次学习和思考的过程。

其次，尽管对职业发展可能并没有帮助，但不论是对内行还是外行来说，证书始终是证明你安全能力的一个有力标签。

下面，我就来分享三个我认为最有价值的证书。为了方便你对比，我把这三个证书的基本信息总结了一张表格。在此基础上，我会重点分析一下，这些证书分别给我们的安全职业发展带来的好处。你可以结合自己的情况，来选择是否考取这些证书。

| 证书    | 特点                      | 难度 | 安全方向 | 考试方法和建议         |
|-------|-------------------------|----|------|-----------------|
| CISP  | 国内安全证书之首                | 中  | 公司防御 | 刷题、<br>考前突击复习   |
| CISSP | 国际上含金量最高的安全证书之一，安全管理者会考 | 高  | 公司防御 | 报培训班、<br>梳理知识框架 |
| OSCP  | 攻击渗透方向上非常实用的证书          | 高  | 攻击渗透 | 刷题、<br>锻炼身体     |



🔗 **CISP** (Certified Information Security Professional，注册信息安全专业认证) 的考试普遍反馈难度不高。不过我认为既然主动去考证了，目标就绝不仅仅只是考试通过，而是以学习和自我提升为主要目的。在内容上，CISP 整理的还是很完善的。而且 CISP 强制培训，在培训过程中，通过讲师的介绍，同样能够学习到不少理论和实践的内容。

在内容上，🔗 **CISSP** (Certification for Information System Security Professional，信息系统安全专业认证) 会比 CISP 更丰富一些，不仅包含一些国际性的政策和框架，还包含诸如物理安全等更偏向运维的内容。另外 CISSP 不存在题库，它的初衷就是希望你不仅仅只是去背教材，而是能够自主梳理知识，并且深刻理解安全。因此，学习 CISSP 不仅能拓展你的知识面，还能帮助你进行自我总结和提升。

CISP 和 CISSP 是更偏向公司防御的证书，而🔗 **OSCP** (Offensive Security Certified Professional，安全攻击专业认证) 是专门针对攻击渗透的证书，最近也比较热门。如果你在自主训练时觉得缺乏明确的方向，其实可以尝试通过考取 OSCP 证书来获得指导。另外，CTF 比赛竞争还是比较激烈，拿到名次也很难。因此，我认为可以将 OSCP 作为 CTF 之外的另一种选择，只要拿到了 OSCP 证书，同样能够证明你的攻击渗透能力达到了可以实际运用的水平。

## 安全资讯

最后，我还想推荐 3 个比较常用的资讯网站，🔗 **FreeBuf**、🔗 **安全客** 和 🔗 **安全牛**。这些网站每天会更新一些安全新闻和学习资料，你可以通过它们快速查询最新的行业动态。我个人一

般是利用休闲时间，来阅读这类网站上的内容。我会先快速地浏览一下标题，找出一些感兴趣的内容进行了解。如果遇到某些特别感兴趣的知识点，想要深入挖掘，我会再搜索其他的相关资料来补充学习。

## 总结

我觉得无论跟随哪个课程进行学习，都不可能学完所有的安全知识。所以，在学习安全的路上，自学是我们不断精进的主要方式。

我的经验是：书籍能够帮助你入门，并且指导你进行防御建设；实战演练是掌握安全渗透技巧的唯一途径；安全证书一方面能帮助你整体的安全知识进行全盘梳理，另一方面也是你个人安全能力的一个证明；安全资讯是帮助你掌握安全动态，发现新知识点的一个不错途径。

想要学好安全，没有什么捷径可以走，唯有多练多看。因此，对于安全的学习，我不建议你在前期花过多的时间去做基础知识储备，那容易变成纸上谈兵。**我更建议的是，当有了一定安全基础之后，你要找机会尽快投入到实际的演练或者工作中。**在实践的过程中，你再对遇到的困难或者知识盲区进行有针对性的学习。另外，在积累实际经验的过程中，周期性的自我总结，以及对知识进行系统梳理，也能很好地推动我们的个人成长。

## 思考题

最后，你可以在留言区讲一讲你的**自学心得，分享一些你的学习资源。**

如果有收获，欢迎你把文章分享给你的朋友。我们下一讲再见！

# 关注极客时间服务号 每日学习签到

月领 25+ 极客币

【点击】保存图片，打开【微信】扫码>>>



© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 加餐3 | 职业发展：应聘安全工程师，我需要注意什么？

## 精选留言 (3)

写留言



王二宝

2020-02-21

感谢老师持续不断的加餐！

展开 ∨



1



leslie

2020-02-21

本期专栏终于出来了，课程留言中多次问及老师何时出此专栏，近年多次典型的安全事件爆出，引发了国内不少企业对于安全的重视。道哥的个人经历和极客时间的二叉树视频看过无数次，其个人履历同样激励了无数的后来者。

安全方面的书籍有读过一些：去年国内的运维大会就有DevSecOps的演讲，听完触动很大。改变了我对于运维的认识和高度，系统、网络、安全在运维这块本在资源方面本就...

展开 ∨



1



qq



2020-02-21

证书对找工作没什么用么。感觉好多JD都会说通过CISP、CISSP优先考虑

作者回复: 对筛简历可能还是有用。但实际面试和评价的时候, 没人会把这一项考虑进来。至少互联网行业内是这样, 国企或者金融相关的, 可能会有这方面政策要求, 也许是个加分项。

